CLAIMS

What is claimed is:

Sub Q3

1. A method for creating a secure script, comprising:

a) generating a hashed value for at least one executable command in the script;

b) signing the hashed value to create a signed hashed value; and

c) appending the signed hashed value to the script.

2. The method of claim 1, wherein generating a hashed value for at least one executable command in the script comprises providing the executable command as a key value that is input to a mathematical function, computing the mathematical function, and providing as output from the mathematical function the hashed value.

3. The method of claim 1, wherein signing the hashed value to create a signed hashed value comprises encrypting the hashed value.

4. The method of claim 3, wherein encrypting the hashed value comprises encrypting the hashed value using a cryptographic key.

5. The method of claim 4, wherein encrypting the hashed value using a cryptographic key comprises encrypting the hashed value using a public encryption private key.

6. The method of claim 5, wherein the script is component in a World Wide Web document downloaded from a HyperText Transfer Protocol server to a client for execution thereon.

7. The method of claim 1, further comprising encrypting the script, including the signed hashed value appended to the script to create an encrypted script.

8. The method of claim 7, wherein encrypting the script comprises encrypting the script using a symmetric encryption key.

9. A method for securing a script, comprising:

a) computing a hashed value for each executable command in a script;

b) encrypting the hashed value for each executable command in the script; and

c) appending to the script the encrypted hashed values for each executable command.

10. The method of claim 9, wherein encrypting the hashed value for each executable command in the script comprises encrypting the hashed value for each executable command with a public encryption private key.

11. The method of claim 10, further comprising signing a control program, comprising the script and a public key corresponding to the private key, to keep hidden the public key.

12. The method of claim 11, wherein signing the control program comprises encrypting the control program using a second public encryption private key.

13. The method of claim 12, wherein the control program is an ActiveX control in an application program.

14. The method of claim 13, wherein the ActiveX control is in a HyperText Markup Language (HTML) document.

15. The method of claim 14, wherein the HTML document is downloaded from a HyperText Transfer Protocol (HTTP) server to a HTTP client.

16. A method for executing a script, comprising:

a) computing a hashed value for each executable command in a script;

b) decrypting an encrypted hashed value appended to the script for each executable command in the script to obtain a decrypted hashed value for each executable command in the script;

c) comparing the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

d) executing the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

17. The method of claim 16, wherein the script is an encrypted script, further comprising decrypting the encrypted script with a symmetric encryption key to obtain the script.

18. The method of claim 16, first comprising verifying a public key cryptography signature associated with a control program comprising the script.

19. The method of claim 16, further comprising repeating a and c each execution of the executable commands in the script to prevent dynamic modification to the script.

20. The method of claim 16, wherein the script is in a HyperText Markup Language (HTML) document.

21. The method of claim 20, wherein the HTML document is downloaded to a Hypertext Transfer Protocol (HTTP) client from a HTTP server.

22. The method of claim 21 performed by an ActiveX control in the HTML document.

23. An article of manufacture comprising a machine accessible medium providing a plurality of machine readable instructions, wherein the instructions, when executed by a processor, cause the processor to:

a) compute a hashed value for each executable command in a script;

b) encrypt the hashed value for each executable command in the script; and

c) append to the script the encrypted hashed values for each executable command.

24. An article of manufacture comprising a machine accessible medium providing a plurality of machine readable instructions, wherein the instructions, when executed by a processor, cause the processor to:

a) compute a hashed value for each executable command in a script;

b) decrypt an encrypted hashed value appended to the script for each executable command in the script to obtain a decrypted hashed value for each executable command in the script;

c) compare the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

d) execute the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.

25. An apparatus, comprising:

means for computing a hashed value for each executable command in a script;

means for encrypting the hashed value for each executable command in the script; and

means for appending to the script the encrypted hashed values for each executable command.

26. An apparatus, comprising:

means for computing a hashed value for each executable command in a script;

means for decrypting an encrypted hashed value appended to the script for each executable command in the script to obtain a decrypted hashed value for each executable command in the script;

means for comparing the computed hashed value for each executable command in the script with the corresponding decrypted hashed value for each executable command in the script; and

means for executing the executable commands in the script if the computed hashed values for the executable commands in the script are the same as the corresponding decrypted hashed values appended to the script for the executable commands.